Current Tipe Graph Region Congress Cong

	Common Origination and		Direct Loans Servicing System	Direct Loans Servicing System	T	1				Debt Management Collections System	Federal Family Education	n E-Application To		Electronic Record	s Financial			Grant inistration and yment System	uman Resources	Information for Financial Aid	Institutional	Multiple Data Entry System/Central Processing	National Student Loan Data	<u> </u>	Ombudsman System	Postsecondary		Student Aid Internet	SFA-PIN
	Disbursement			(eServicing)	Direct Loans Consolidations	Consistent Answers	Datamarts				Loan	Participate		Management	System		Adm Pay		Modernization	Professionals *	Assessment Model	System	System			Educational Participants System	EDPUBS students.	Gateway	
SFA - Single Sign-on	COD	Pel/RFMS DLOS-FAPs	DLSS - Non-Student	eServicing Initiative: Direct Loans Servicing System	DLCS - Non Student	Consistent Answers		Credit lanagement Delinquent Los		DMCS	FFEL	E-App	ED-Express EDNET	ERM	FMS	e799	Financial Report (Forms 2000)	GAPS Jam Pe	Netsourced Applications: Applications: Application Jamcracker Platform, orform.com, Saba (2.9.X) (3.0)		IAM	MDE/CPS non-student	NSLDS-FAP	NSLDS-Student	octs	PEPS		SAIG / TIVWAN	eCB (eCampus-based System) CPS (Central Processing System) - Students
Data Collection Status  General  Contacts	Complete  Common Origination and Disbursement	Peti originations 8. disbursements (net 12/02)  Di. originations and disbursements	Complete  Direct Loan payments, servicing	Complete  User: Direct Loan Servicing (eServicing)	Complete  Complete  Direct Loan Consolidations	Complete  Customer Call Center (Q3FY02)	Complete	Complete Complete	Complete	Complete	Complete  Federal Family Education Loan	Complete	Availing flootback   Added 2/13/200  Communications of school data to SFA   area network	Complete  Complete  Submissions		Planned add-on to FMS	Planned add-on to FMS cu	uest payments and access to ment grant and ayment data  Sing	Complete Complete Complete Commance Mangement Saba - Learn Saba - Lear	mance t General into for	Complete  Data for compliance for Aid Administration	Complete	Complete Reporting and other services	Complete  Reporting and other services	Complete	Complete  Maintains eligibility, certification, demographic, financial, review, audit & delault rate data about Schools, Lenders, Guarantors	Complete 99 Complet  Former Publication Oxdering	Awaiting NCS feedback	Allows users to submit. FISSAP Performation, access clampus-Based and occurrence data, and view reports.  View SAR data, Check batch stasss, Make RAD requests, Request renewal application duplicate, PIN requests
IPT contact Business Process	Colleen Kennedy  Direct & Pell loan origination and disbursement	Colleen Kennedy Colleen Kennedy  d Pell originations & Direct loan originat disbursements		Robert Laurence	Robert Laurence Direct Loan consolidations	Colleen Kennedy  Call center/customers	Mike Bruce 1	Mike Bruce Mike Bruce	Mike Bruce	Robert Laurence	Robert Laurence	Colleen Kennedy	Mike Bruce	Mike Bruce	Michele Selvage	Michele Selvage 799 Submissions (planned)	Michele Selvage S  LEAP and SLEEP Loans (planned)  Gran	andra Fowler its Management	Mike Bruce Mike Bruce	Colleen Kennedy	School Case/Aid Eligibility	Robert Laurence	Sandra Fowler	Sandra Fowler	Sandra Fowler	Pam Eliadis	Colleen Kennedy Neil Satt	r Sandra Fowler	Colleen Kennedy Robert Laurence  Campus-Based Programs
Business Owner System Owner	Kay Jacks 202-377-4286 Kay Jacks 202-377-4286	Kay Jacks 202-377-4286 Kay Jacks 202-377-4 Kay Jacks 202-377-4286 Kay Jacks 202-377-4		Dan Hayward (202) 377-3207	Denise Leifeste, (202) 377-3293	Kay Jacks 202-377- 4286 Kay Jacks 202-377-	Anna Allen, (202)	nifer Douglas Jennifer Dougl	Anna Allen, (202) 377-	Jennifer Douglas Gary Hopkins	Jennifer Douglas	Kay Jacks	Kay Jacks	Kay Jacks Cheryl Queen, 202	John Reeves Paul Stonner, (202)		John Reeves Paul Stonner, (202)		in Thomas 202-377- Calvin Thomas 2			Jennifer Douglas Jeanne Saunders (202) 377-3246			Debra Wiley, (202) 377-380	0	Kay Jacks		Kay Jacks 202-377-4286 Jennifer Douglas Milton Thomas (202) 377-
System Manager (SM)	Sandy Whitmire 202-377-3136	3/7-3126	Dan Hayward (202) 377-3207	Dan Hayward, (202) 377-3207	Denise Leifeste, (202) 377-3293	None ?		ott Smith, 202- 377-3279 Scott Smith, 20 377-3279 377-3279		Brian Sullivan 202-377-3254		Rana O'Brien 202-377- 4312		Len Matheny	Shirley Singleton, (202) 377-3491		Shirley Singleton, Ro (202) 377-3491 2	ger Goodson, Joh 02-401-0108	3011 3011 in O. Olumoya 202- 377-3534 John O. Olumoy 377-3534 377-3534	a 202- Colleen Kennedy, (202) 377-4119	John Hill, (202) 377- 4377	Nancy Reynolds (202) 377-3245 (CPS) Maria Carmona (202) 377-3884 (MDE)		46 Barbara Cobbs, 202-377-3555	Corwin Jennings 202-377- 3291	Rana O'Brian, 202-377-4312 Nita Washington, 202-708-	Lynda Folwio 377-351		3182 Richard Coppage, (202) 377-3174 Jeanne Saunders, (202) 377-3246 Milton Thomas (202) 377- Voone Somerville, 202-
System Security officer (SSO) Logon (Credentials)	Ellis Williams, 202-377-3048	Theresa Vaughan, 202-37- 3103 Donnell Dorsey, 202- 3131	Schonda Piper (202) 377-3275	Schonda Piper, 202-377-3275	Yvette Payne, (202) 377-3295		377-3320 Scho	onda Piper, 202- Schonda Piper, 377-3275 377-3275	3320 Willie Sutton 202-377-	David Yang 202-377-3256	David Yang 202-377-3256			Paulette Jones	(202) 377-3318	(202) 377-3318	(202) 377-3318	800	ott Bone (703) 947- 1236 Scott Bone (703 1236	(202) 377-4336	John Hill, (202) 377- 4377	Yvorne Somerville (202) 377-3247	Barbara Cobbs, 202-377-3555	5 Lynn Alexander, (202) 377-3546	3291	Nita Washington, 202-708- 6566	377-351	, 202 Tawanda Hampson, 202 377-3575	Milton Thomas (202) 377- 3182 Yvonne Somerville, 202- 377-3247
Username	COD Login	Pell ID, TG (TIVWAN) Number DLO Login ID	DLSS Login IBM (System lovel): 3. Alchenumeric	DLSS Username	DLCS login ID OR SSN+first two letter FN+DOB	Employees - TBD; Students - SSN (under review)	EDNet user ID E0	DNet user ID EDNet user ID	D EDNet user ID	DMCS/FFEL Username	DMCS/FFEL Username	OPE ID + TIN (taxpayer identification number)		ERM Usemame	FMS Username	FMS Username	FMS Usemame C	BAPS Userid Ja	amcracker Userid Jamcracker Us	serid IFAP Usemame	IAM Usemame	CPS UserID	NSLDS Userid	SSN + First two letters of last nam + Date of birth	OCTS Username	PEPS Username (Citrix Username)	Office of Postsecondary None Education ID (OPEID)		SSN, First two letters of last name, Date of Birth last name + Date of birth
Minimum length	8	ID:6, TG: 7	IBM (Application Level FARS): 4 Alphanumeric OpenMVS (System level): 3 Alphanumeric On-Line (Processor Code): 4 Numeric IBM (System) (syst): 8 Alphanumeric	1 character	5	9	2	2 2	2	3	3	OPEID - 8 digits; TIN 9 digits		none	No minimum length configurable	No minimum length configurable	No minimum length configurable		1 1	8 char	2	6 alphanumeric		19 numeric+2alphanumeric+8numeric	2	4	8 n.a.		9 9 numeric+2alphanumeric+8n umeric umeric
Maximum length	8	ID:6, TG: 7	IBM (Application Level FARS): 4 Alphanumeric OpenMVS (System level): (7) On-Line (Processor Code): 4 Numeric	No limit	8	9	256	256 256	256	7	7	n.e.		20 characters	No maximum length configurable	No maximum length configurable	No maximum length configurable		20 20	8 char	256	8 character	unlimited (256 character)	19	32	8	8 n.a.		9 9
Syntax rules	First two letters of FN + First four letters of LN + Last two numbers of school OPEID number	ID: Only digits, TG: TQ[5 6]+4 3 logon attempts ut digits locktout	IBM (Bystem level): Alphanumeric IBM (Application Level FARS): Alphanumeric OpenMVB (Bystem level): Alphanumeric On-Line (Processor Code): Numeric	Must not be blank	alphanumeric, first letter of first name, up to 5 letters of last name and 2 numeric characters		first name +last first name	a + first initial of Code + first initia st name +last name name	al of # first initial of first name +last name	Must not be blank, No special characters	Must not be blank, No special characters	OPE ID never changes for an institution; TIN may change. PEPS stores prior TINs		20 upper or lowerce characters except to following: "N[]:: =,+"?<: user name canno consist solely of periods and space	First name initial + A last name, Some stil t have "ED" in front.	First name initial + Il last name, Some still have "ED" in front.	First name initial + last name, Some still have "ED" in front.	sp I	Alphanumeric (no saces but you can have a period or usersore in the username)  Seword (Allows for Password (Allo	can Letter First Name + First 6 char Last Name + Number; Admin - no rule	First Initial of First Name + Last Name	NCS Pearson user lds consist of a 3- or 4- letter department abbreviation followed b 3 or 4 digits, usually an employee number. Must not be blank.		Must not be empty, 9 characters long	First letter of FN + LN	2 Letter Office Code (e.g., EN, EI, OC) + First letter of FN + LN	Numeric n.a.		Must not be empty, 9 characters long characters long
Password/PIN/other	COD Password	RFMS Password DLOS Password	DLSS Password  IBM (System Level): 30 days	DLSS Password  Siebel (i.e. Oracle) Passwords do not	DLCS Password OR SFA PIN	Employees - TBD; Students - PIN (under review)	Password must be Pas	M Datamant Password Password  M Del Loan Datam Password  Password must be Password must	be Password must be rest	DMCS/FFEL Password	DMCS/FFEL Password	None		ERM Password	30 days (Some still	FMS Password  30 days (Some still 60 or 90 days). If	30 days (Some still	NPS Password sm	art card, biometric, smart card, bion etc.) etc.)	netric, IFAP Password ine, 15	IAM Password	CPS Password  No Limit, but will expire after 90 days of inactivity.	NSLDS Password	SFA-PIN	OCTS Password	PEPS Password (Citrix Password)  For Citrix web users 90-	N.a. None		SFA-PIN and TG number SFA-PIN  Expire after 6 months of Expire after 6 months of
Lifetime	60-days, users sent message to change password	o 90-day reauthenticate with TIVWAN ID and Password	IBM (Applications Level FARS): 30 days Open/VMS VAX: 30days LAN (UPIC): No expiration LAN (RSSC): 30 days IBM (System level): 6 Alpharametic	expire; NT Password will expire every 3i days (administered by AFSA)	0 30 days	Lifetime of user, does not change	thereafter, every 90 there	t for initial use; eafter, every 90 days days	se; for initial use; y 90 thereafter, every 90 days	Expires after 6 month of inactivity	Expires after 6 month of inactivity	n.a.		Never Expires	user is inactive for 3	10 user is inactive for 30 days, account is locked.	user is inactive for 30	days 60 c	a, 30 days, 45 days, days, 30 days, 45 days, 3 mo, 6 mo, 1 60 days, 3 mo, 6 year year	5 days, mo, 1 Forever	Forever, no limit	Must be changed every 30 days.	120 days	Expire after 6 months of inactivity else valid indefinitely	Lifetime	days; For direct access users no limit	Na. na.		inactivity; else valid inactivity; else valid indefinitely indefinitely
Minimum length	8	4	IBM (Application Level FARS): 5 Alphanumeric OpenMVS (System level): (?) Alphanumeric On-Line (Processor Code): 6 Numeric IBM (System Issue): 9 Alphanumeric	1	8	4	1 character 1	1 character 1 character	1 character	5	5	n.a.		5	Configurable, 5	Configurable, 5	Configurable, 5		6 6	5	8	5		4	6	any	Na. n.a.		4 4
Maximum length	8	15	IBM (Application Level FARS): 5 Alphanumeric OpenMVS (System level):(7) Alphanumeric On-Line (Processor Code):(?) Numeric	No limit	8	6	none defined n	one defined none defined	I none defined	8	8	n.a.		14	Not configurable	Not configurable	Not configurable		16 16	8	8	8	19	6	6	field limit (256)	Na. na.		6 6
Syntax rulies	6 alpha characters and 2 numeric characters	4-15 alphanumeric	IBM (System level): Alphanumetic, no dualse charactures BM (Application Level FARS'): 8 Alphanumetic OpenMVS (System level); ("Alphanumetic On-Line (Processor Code); (") Numeric In the event that a user stamptes to gin three consecutives times with an incorrect password, the access to the system i automatically evoked.	Must not be blank	Password - Must not be blank, mus be different than last 3 ones, must kept for at least a day. SFA PIN used for Application Satus Look-Up and e-signature of LC Prevency. Syo Notes on the LC Web Application, PIN does not expire, however, if yo have requested a new PIN, only you new PIN can be used.	be  p   numeric  -	characters, spaces char	y not be blank, May not be blank, alphanumeric alchers, spaces on OK	nik, May not be blank, alphanumeric characters, spaces OK	Must be not blank, No special characters	Must be not blank, No special characters	n.a.		14 upper or loweros characters except to following: "/(  :  =,+"? <: user name canno consist solely of periods and space	sse he A No t	No	No	Alp	hanumeric, at least ne letter and one number	t least Users & Admin, one None	System generated; contains alpha, numeric, control characters	ED and Contracon logging or via CICS or TBD: No spaces. Not Cade Servisive. Users are instructed in the Contract of the Contract of the Contract School personnel logging or via Contract Contraged every 120 days, No special characters, Passessords may be any word found in the decionary Ubers are instructed ont to use words that may be offerable or obscione.	Stored in RACF	Must not be blank, must be digits	6 characters; 3 must be numbers	none, new password nules will be: 8 characters min's 4 char max, meet three of the following (one or more uppercase letters, one or more lowercase letters, one or more non-ealpha characters), cannot have been used in the previous 13 password cycles	Na. na.		Must not be black, must be Must not be blank, must be digits
Previous passwords stored	Yes, Past 3	Yes, the last 2	Yes. Password Reuse rules: IBM: Cannot use 5 previous passwords; OpenVMS VAX: Cannot use previous passwords for up to 1 year	s No	Yes, last 3	No, user keeps same PIN unless a new entity is created	Not enforced N	lot enforced Not enforced	Not enforced	Yes	Yes	PEPS stores prior TINs		No	No	No	No		max 3 changes per Yes, max 3 changes session  practic Database  Oractic Database  Oractic Database	No ase	na.	Yes, Once a contractor or ED employee's CICS or TSO password has experied, it may not be used again until 12 other passwords have been used. Edcornect32 users expired passwords may not be used again until at least 20 other passwords have been used.		No	No	No	Na. na.		No No
System where credentials are stored	Oracle database at TSYS	Pell - SQL Server 6.5 Database for ID/Authentication; RFMS - RACF 2.4 VSAM repository for roles		Siebel (i.e. Oracle) and NT Server	User file with one-way (Hash) encryption, secured by CA-Unicents TNG Security Subsystem. Unix Password file not shadowed.	Consistent Answer user store (oracle); SFA PIN database	MicroStrategy M repository	icroStrategy MicroStrategy repository	MicroStrategy repository	RACF	RACF	eAppPEPS			Oracle Financial (Application table)	Oracle Financial (Application table)	Oracle Financial (Application table)		edentials to login to (credentials to lo saba/Perform are Saba/Perform de in Oracle) LDAP stored in Oracle adentials to login to ncracker are stored Jamcracker are		IAM user database		RACF R4 (2.2) on NSLDS mainframe; VSAM files	SFA-PIN site	OCTS repository	PEPS Oracle DBMS	Na. n.a.		SFA-PIN and TG number SFA-PIN site
General															Length of password limited by field length	is Length of password is h limited by field length	Length of password is limited by field length	Jan	in LDAP) in LDAP)	sicred				PIN not retrievable					PIN not retrievable PIN not retrievable
Guest accounts	No	No	No	No	No	No	No, SFA user have separate user lds, GA/Lender use group lds	No No	No, SFA user have separate user lds, GA/Lender use group lds	Yes	Yes	Maybe, Trainer Ids available to allow demo of the site, but these Ids do not access real		No	No	No	No		N/A N/A	No	No	No	No	No		No	n.a.		No No
Disable when inactive	Yes, manually by System Administrator (global) or School Administrator (restricted to school)	After 90 days	Yes, after ??? months of inactivity	Plans are to follow current AFSA NT administration policies for NT account inactivity. Siebel ids are disabled manual by the administrator.	By Yes, after 30 days (?)	77	Yes, after 60 Y	Yes, after 60 Yes, after 60 minutes minutes		Yes, after 15-30 minutes session timeout and	Yes, after 15-30 minutes session timeout and	Yes, E-App uses the Oracle Listener File in PEPS to grant access. Users removed when PEPS updates this file with closed schools		Yes, when administrator notific	Yes, 30 days	Yes, 30 days	Yes, 30 days		Manually by Manually b administrator as administrator requested.		No accounts inactivated to date	After 90 days of inactivity CICS/TSO userids removed on a weekly basis	RACF allows three failed logor attempts before account blocked	n Yes, after 6 month	Yes, Manual as credential compromised or user depart Ombudsman office	s No	n.a.		Yes, after 6 month Yes, after 6 month
Credential date elements	Username + Password	User ID and password (and TG for schools)	Userid, Password	Credentals (i.e., oas dements) used to logon: NT User Id NT Password Phone Id (switch Logon) Siebel User Id Siebel Password DLSS Processor Code	Username, Password, SFA PIN		EDNet user ID and EDN password	Net user ID and EDNet user ID a password password	EDNet user ID and password	User ID and password	User ID and password	OPE ID + TIN		UserID provided to user by ED	Usemame (First name) Initial + Last name) Password	ne Username (First name , Initial + Last name), Password	a Usemame (First name Initial + Last name), Password	Com	epany name, user id, Company name, password password	Username and Password validated against Oracle table	Username and password	Userid, Password	Username and Password validated in RACF	Username, PIN (Username consist of SSN, DOB, LN)	S Username, Password	Username, Password	n.a.		PIN, TG, SSN, First 2 characters of last name
Single or multiple logans for one user	One	Pell ID and TIVWAN ID have many-to-many relationship	Mutiple, to keep DBA functions separate from normal programmer support trouble shooting Production Applications problems.	Multiple logins for a user	Single	Single	Single	Single Single	Single	Single	Single	Single		Single	Single (Multiple Role for 1 UserID possible	s Single (Multiple Roles e) for 1 UserID possible)	Single (Multiple Roles ) for 1 UserID possible)		Single Single	One Logon, per registration entry; Self registration except for	One	Single	Single	Single	Single	Single general; some users may have multiple logins	n.a.		Single Single
Different credentials for user groups	No	Same access creder for all Valed users or Yes are: AFAO, CAR, O. CSR, SFAO, TPS, L User, Super User	pt - Production Control	No	Yes	to be determined; based on Slobel capability	No	No No	No	Yes	Yes	No, Schools only		One users can be assigned multiple groups	No	No	No.		No No	2 Groups - Users and Administrators	No	Groups: SFA Staff, Contractor Staff, School Staff	TIVWAN registration provides roles within system	i No	Yes, User Group and Systen Administrator	No, 3 database roles (Add, Change, View) and multiple application user classes	n.a.		No No
Encryption of credentials	Yes, 2-way	SSL 128-bit for SSL 128-bit for communications communications	Yes, credentials are stored in an encrypted state.	No	Yes, one-way (Hash)	1-way	Yes	Yes Yes	Yes	Yes	Yes	No		NT default encrypti	on Yes, One-way (Hash	n) Yes, One-way (Hash)	Yes, One-way (Hash)	Si	HA, LDAP and DB SHA, LDAP an	d DB No		Yes, redentials are stored in an encrypted state. The Security Module I is used in conjunction with user authentication for encryption, decryption, hashing, and pin generation. This Ite has incorporated Version 3.0 of RSA BSAFE Cryptotographics libraries and SHA-1 to provide secure encryption, decryption, hashing and pin generation routines.	Passwords encrypted in RACF No encryption server to mainframe communication	F; Yes, two-way	No	No	n.a.		Yes, two-way Yes, two-way
Comments	SSL browser session, Logs to record user activity	Communications Pa- NT/SM4 4.0, CAContricting 4.1s. NT Security SPAB - T/CPHP 2.4, OCD 4.1 Security Colores TMD Security Colores TMD Security Colores TMD Security Colores TMD		Oracle passwords are encrypted at the server, such that users cannot open Orac connections through another development tool (i.e. MS Access). User groups includ. Customer Service Representatives, 5F, Statt, Development Programmers, Production Control, Systems Analyst s	de	Centralized user admin at VDC	No Audit trails N	o Audit traits — No Audit traits	s No Audit trails			E-App is a feeder system with data stored in PEPS. Schools recertly once every 6 years. Schools use eApp to update their PEPS information as needed						cred	Saba/Perform Saba/Perform Saba/Perform Saba/Perform the Cracle DB (encrypted) (encrypted)	ored in attempt; System logs	Initial password emailed to users	ISFA PNI used for Renneal Applications on the Web PNI good will deached by the user, or systems administrate.	Communications: Internal via EDNET, catemal via Internet, 128-bit SSL enception on Internet, FAP web server passes credentiatio RACF to authentication				n.a.		3 user groups (ReacYYMM/5)ubmt)
User management  Enrollment	COD enrollment	SAIG online agreement Direct Loan Enrollm	nt	User Administrators create accounts manually. CSRs do not have access to	Direct Loan Enrollment	Enrolled using Siebel by VDC System		M Datamart Del Loan Datan		DMCS Enrollment	DMCS Enrollment				Oracle Financials	Oracle Financials	Oracle Financials EDC	APS enrollment Jam	cracker provisioning Jameracker provi	aioning IFAP Registration	Request royted to Systems Manager and Administrator to	The System Administrator assigns Usernames	SAIG online agreement	SFA self service PIN web site		ED ADP Access Authorization, 1000 userids; 800 active ED users: 400	None		SAIG online agreement & SFA self service PIN web
		DEMO. I N EN MI Engrer VDC Mid Range Enrol		charge, add or modify users.		Administrator based on valid enrollment form	Enrollment	Enrollment Enrollment	Enrollment	FFEL Logon Request - LN, FN, MI, Telephone, Protition/Title I lee Generic	FFEL Logon Request - LN, FN, M, Telephone, Position/Title, Use Generic Profile yin, Region, ED	i,			Enrollment	Enrollment	Enrollment EDC	No.	usemame entered No, username e	online online	add new user/employee		Probationary NSLDS - LN, FN	4,		external via Citrix web, Oracle Roles ID/authorize			site site
Enrollment data elements	COD User Enrollment process COD Letter, User information, school administrator sets up school users; VDC Mid Range	Signature/date, Supervisor Application Name (V SFA), VDC System n	O, Cc, me, you		VDC Mid Range	VDC Mid Range	VDC Mid Range VD	IC Mid Range VDC Mid Rang	je VDC Mid Range	Group, Action, Clearance Submit Date, SSN, Collection Agency Code, Collection Agency name, Provincements, PACE	Group, Action, Clearance Submit Date, SSN, Collection Agency Code, Collection Agency name, Provincements, PACE	nn PEPS data/application by school		User ID's are creat by Dept. of ED and added to system b System Security Add	y FMS Registration	VDC Mid Range; FMS Registration	VDC Mid Range; FMS Registration	in U the filling	II. Jamcracker/Saba semame created ough external user through external user gout data gathering filling out data garneous form.  In Jamcracker Saba in U.I. Jamcracker Saba i	r(Saba FN, LN, E-mail, and Institution/ I user Organization, City, thering State, FAP Group	Request to System Manager, no specific form	VDC Mid Range	Mother's Maiden name, DOB, ED Loan Status, RACF Profile User NSLDS - Current NSLDS ID, Current FSLD, LN, FN, MI, Title, Bus Address, Bus Telephone, SSN, Mothers Maiden Name, DOB, Principal Operating Component	N. SFA-PIN - SSN, LN. FN, MI, DOB Street Address, City, State, ZIP, email address, security pass- phrase		VDC Mid Range; GA, Contractors, SFA employees, Schools have enrollment forms on web site	n.a.		SFA-PIN SFA-PIN
Username creation automater  System generates initial	No, manually created Yes	VDC determines username password managem part of LO Office application No, user provides temp	The Security Administrator assigns Usernames  The Security Administrator assigns the initial coseword	The Security Administrator assigns Usernames  Security Administrator assigns the initial	No, manually created based on rule  No, assigned by SSO	to be determined		Yes Yes	Yes	No, Sysadmin assignees usemame	No, Sysadmin assignees username Yes	System generated as part of school eligibility determination		Manual, generated system administrat	No (Prod support team creates account)	No (Prod support team creates account)	No (Prod support team creates account)	ger 9	is - corringuitable - personne - corringuitable - personne - perso	tem on #2) vord Users - Yes, see above	Manual by System Administrator	The Central Security Administrator in Technical Support assigns user lds.  System Administrator assigns the initial password	Initial Password provided to	Yes  Yes, but chanceable	Usernames created by System Administrator Password created by System	Manual by administrator  Created manually	n.a.		Yes Yes Yes tut chanosable Yes, but chanosable
Password  User is forced to change initial Password  Removal	Yes	password Yes	Yes	password for Siebel; Yes for NT. No for Siebel, Yes for NT.	No, assigned by SSU Yes	Students - No, SFA-PIN		Yes Yes	Yes	Yes	Yes	generated No		Yes	Yes	Yes	Yes		165	Yes - see above	No No	Yes	user User changes on website; update processed manually inte RACF	ves, but changeasse to No, mail via USPS to recipient	Administrator No	User sent Password by email; asked to change but not required to	na.		Yes, but changeable Yes, but changeable  No, mailed via USPS or email to recipient Roughly Rou
Average time before removal	As requested, within minutes by administrator	-24H		One day	Immediately	to be determined	Immediate	Immediate Immediate	Immediate	less than 72 hours	less than 72 hours	Within 24 hours		1 day from time o notification to syste security administrat	r m ?	?	7	Rea	alfime, as requested Realtime, as req by Administrator by Administrator	uested As requested	No users removed	Whenever an ED employee with access to the CPG no longer requires access to the system, ED notifies access to the system, ED notifies access to the system, ED notifies access. When NCS Reason, the I harmon Resources Department has processed in place in the event of a full-time employee's voluntary summarion or relocation. Shortly after the first activation of the state of the st		Immediately	2 minutes once revoked	2 minutes; Upon request by administrator	n.a.		Immediately Immediately
Manual or automated	Manual administration	Semi-automatically	The Security Administrator also has the ability to remove a us from the system manually (i.e., when a compromise is	Manual. Security Administrator also has t ability to remove a user from the system manually (i.e., when a compromise is	he Both (3 attempts to login with wrong	g to be determined	Manual	Manual Manual	Manual	Manual	Manual	Manual		Manual	Manually	Manually	Manually	n n	fanual by system Manual by sys	tem Manual by DBA	Manual removal	the employee termination is involuntary, these departments are called immediately and an e-mail will follow.  The Security Administrator also has the ability to semove a user from the system manually (i.e., when a compromise is suspected).	Manual from RACF	7	Manual by System	Manual	n.a.		? ?
			suspected).	manually (i.e., when a compromise is suspected).	password - locks account)								I						administrator administrati			a compromise is suspected).		1	Administrator				

Cument System Logan Analysis
Sing- Graph Requirements Test
Single Sign- on Requirements
Single Sign- on Requirements

				T.															,											1	T
	Common Origination and Disbursement			Direct Loans Servicing System	Direct Loans Servicing System (eServicing)	Direct Loans Consolidations	Consistent Answers	Datamarts			Debt Management Collections System	Federal Family Educatio Loan	n E-Application To Participate	ED-Express	EDNET Electr Ma	onic Records inagement	Financial Management System			Grant Administration and Payment System Human Resources Modernization		Information for Financial Aid Professionals	Institutional ssessment Model	Multiple Data Entry System/Central Processing System	National Student Loan I System	Data	Ombudsman System	Postsecondary Educational Participants System	EDPUBS students.gov	Student Aid Internet Gateway	SFA-PIN
SFA - Single Sign-on	COD	PelVRFMS	DLOS-FAPs	DLSS - Non-Student	eServicing Initiative: Direct Loans Servicing System	DLCS - Non Student	Consistent Answers	Financial Partners Man	Credit Deline	uent Loans CFO	DMCS	FFEL	E-App	ED-Express	EDNET	ERM	FMS	e799	Guaranteed Agency Financial Report (Forms 2000)	Netsourced Applications: GAPS Jamcracker Platform, Perform.com, Saba (2.9.X)	Netsourced Applications: Jamcracker Platforn Perform.com, Saba (3.0)	i, IFAP	IAM	MDE/CPS non-student	NSLDS-FAP	NSLDS-Student	остя	PEPS		SAIG / TIVWAN	eCB (eCampus-based System) CPS (Central Processin System) - Students
C for fiser groups, where stored 1.	COD Roles - Rel. 1.0 4 School level, 1 School Administrator, Rel 1.1 25 School levels. Roles and credentials in TSYS Oracle DBMS	I bl 1 RACF		User groups and identifies are stored on the Alpha 8400 housed in the ACS Rockville Computer Center, and for FARS of the VDC IBM mainframe (Due to be refired by June, 2002).	on Courtey and the FADC on the MDC IDM	In user file , Unix password file not shadowed	t Consistent Answers repository	User Profile Us Repository Re	ser Profile Us repository Ri	er Profile upository  User Profile Repository	y VDC houses them	VDC houses them	PEPS and Oracle Listener File stores OPEID and TIN		NT Pr	imary Domain Controller	Oracle DB	Oracle DB	Oracle DB	Oracle Database and LDAP	Oracle Database and LDAP	Oracle IFAP database o	No groups. Users stored in IAM latabase and IAM lministrator desktop	Users Groups and User Identities are housed in the VDC	RACF	PIN DB (Oracle DB housed at VD	C) Employee file resident within Siebel CRM application	PEPS Oracle DBMS; enrollment papers stored offline	n.a.		PIN DB (Oracle DB housed at VDC) & SAIG System at VDC)
iss word administration automated <sub>c</sub>	Manual usefid creation, passwood reset, disable; User can manage profile, key word, no user password reset	No, Policy, Monitoring and II by Security Administrator a VDC	DS EDS LO ordine web application 6.01	Every user ID has a password associated with I that subherolosis is used forties. The security derivolated used has been assign an intelligeneous The user is required to change in the relative and intelligence of the password at initial system loops. If the user alternity is got in their conscious being with an including password, the light period of the password is set in the password in the pa	password. The user is required to change is his or her password at initial system logor.  If the user attempts to log in three consecutive times with an incorrect password, the access to the system is m revoked. At that time, the user must call the	Yes/No (If user is locked out, SSO must unlock him/her)	to be determined	No, user contacts security official, secu who follows SFA procedures pro	user contacts No, u urity official, sec- follows SFA who pri	ser contacts risy official, security official, who dolows SFA procedures	RACF S	RACF	na.		N	io, manual	No	No	No	Ubers change password online; system administrator can reset password	Users change passwo oritine; system administrator can resi password	d Users can change t Password online	Creation yes	Yes, RACF	Users can change onlin change manually entere RACF	e; to Yes	Manual by System Administrator. Monthly review of password holders to remove invalid users	Manual	na.		Yes Yes
lumber of enrolled users 21	20,000 users - FAPs at schools, Gas, FPs			??	As of August 2002, there will be -700 enrolled users.	77	Students, Others?	Current 85; Future aprox. 4000	100	4 to 6	3,000	3,000	10,000 institutions (5600 domestic and 4400 foreign)			300+ 200	urrent 515, June 02 expect 10,500; peak at 20,000	?	?	12,000 +	12,000 +	5,000 in	00 SFA Employees Case Management	As of Feb. 2002, there are 374 enrolled users at NCS Pearson of which, of which, 88 are temporary employees.	21,346	27,274,093 including other SFA-P sites	N 77	1000 userids; 800 active ED users; 400 external via Citris web	n.a.		27,274,093 including other SFA-PIN sites SFA-PIN sites
ssion management	Timeout if inactive	15 minutes set by IIS		IBM: CICS timeout after 30 minutes of inactivity.  LAN: Timeout after 30 minutes of inactivity.  Open/MS/SVAX timeout after 30 minutes of inactivity.  Ominutes of inactivity on submenus and 20 minutes of inactivity on submenus and 20 minutes of a minutes.  Open/MS/SVAX terminals connected for Development use: (7)	No rules for timeout	??	to be determined	60 minutes 60	O minutes 60	minutes 60 minutes	15-30 minutes depending on user group	15-30 minutes depending o user group	n No		out t	f activity times prowser user, antly set at 60 minutes	io, configurable N	o, configurable	No, configurable	30 minuses	30 minutes	None	No	After 15 minutes of inactivity on TSO and 30 minutes on CICS, users will timeout. In the event that a user attempts to log in 3 consecutive times with an incorrect password, the access to the system is automatically revoked.	Web: 30 minute; Mainfra CICS maintained, 10 min	me: 30 minutes stes	Yes if no key activity in 10 minutes	None	No		30 minutes 30 minutes
ogaut button	Yes	Yes		session timeout. Yes	Closing the application logs out the user	Yes	Yes	Yes	Yes	Yes Yes	Other logout mechanisms	Other logout mechanisms	No, Send button refreshes the web data submission page		logout i head	s handled by a link on the main or page of the web site	Yes (?)	Yes (?)	Yes (7)	Yes	Yes	Yes	No	Yes		Yes	No, auto interrupt from server application via a command link	No	No		Yes Yes
fechanism for session nanagement	User cache in system			n	Oracle maintains session	77	to be determined	Oracle web server Oracle	le web server Oracle	web server Oracle web server	RACF	RACF	None			IIS O	racie web server On	acle web server	Oracle web server	Closing browser window of session	Closing browser windo of session	w Session closed by closing browser	None, Stateless	RACF	Mainframe: CICS	Oracle WAS (Session DB)	Siebel application manager 5.6	Direct access none; Citrix web server	n.a.		Oracle WAS (Session DB) Oracle WAS (Session DB
Concurrent Sessions	Yes	?		n	Yes, Users may logon on to multiple NT Workstations and Siebel applications with the same User Id.	77	to be determined	Yes	Yes	Yes Yes	No	No	No, lockout once one user from a school has logged in		Yes u concu	p to the limit of irrent licenses available	Yes	Yes	Yes	Yes	Yes	n.a.	Yes	No		No	Yes	Yes	n.a.		No No
ccess limited by time	No	No		No	No	77	No	7AM-10PM EST 7AM-	1-10PM EST 7AM	-10PM EST 7AM-10PM EST	No	No	No		Shut di AM Ci	own 10 PM to 4 8AM ST for backups	M-8pm EST, soon 8AM 24x7	1-8pm EST, soon 24x7	8AM-8pm EST, soon 24x7	No, Help Desk available 1 24x7	No, see note to right f exception	or No, Help Desk available 8 - 5	24)(7	No		No, 24X7 availability	No	No	No		No, 24x7 availability No, 24X7 availability
ocess limited by location  Veb or dedicated access	No Web access	No Web access	Web access only	77	Limited to diployed floatition of roll centers in Basernistic, CAnn tilloo, BY (and tilloo, BY (and tilloo, BY (and development locations)  Dedicated	?? Web	No  Employees via SFA-to-the-Internet. Call centers by Dedicated			No No No Both Both	No Dedicated access	No  Dedicated access	No Web			No IHTTPS, SSL 1	No V/PN access for vectain users	No PN access for sentain users	No  VPN access for certain users	No.	No Web	No Web	No Web	No.  These are two mutuals of the logistics of the TS for ED and contrainer seaf—the logistics of the method contrainer seaf—the logistics of the method contrainer seaf—the logistics of the logistics of the logistics of the logistic of th		No  Web and IVR	No  Web and Siebel client	No Web and Direct	No Web		No No Web and IVR
rastructure .	VDC, TSYS						VDC	VDC	VDC	VDC VDC	VDC	VDC	VDC		AI	SP service	see	FMS s	see FMS				lak Ridge National					Web - VDC; Direct Access -			NCS Pearson - PIN NCS Pearson - PIN database; VDC - Web database; VDC - Web
Date Center Location  Hardware platform	HP, Sun, MQSeries	VDC Pell - Compaq 1850R; RFN IBM mainframe	VDC AS HP-9000 T600	AGS - Rockelike; and VDC  Alpha 8400s / IBM Mainframe	ACS - Rockville; and VDC  HP-UX Database server	VDC HP-9000	Wintel (tbd, HP-LIX Oracle 8.x database	Intel, HP, Sun Intel	el, HP, Sun Inte	I, HP, Sun Intel, HP, Sun	IBM 9276-R35	IBM 3390-3	PEPS/EAPP Compaq	HP	Con	npaq DL 380	VDC P V-class and L- class servers			Jameracker Sun Spare	Sun Sparc	VDC Sun, HP (database), database Oracle 8; 2 servers are load balanced by network dispatcher	Intel	VDC  IBM 9672-R74 Parallel Enterprise Server	Web: Compaq 1850R; D IBM 9672 mainframe	VDC; NCS-Pearson	Compaq Prollant 1850R	ED Office  HP; eApp on NT with IIS	VDC IBM, HP	Compaq	Application; SAIG System Application  SEA-PIN: Intal, HP, Sun eCR: ESSO Sun Sparc, HP 9000 V Class Database Server, Compaq D1389 Server D1389 Server
Operating System	HP-UX, Sun Solaris	Pell - NT 4.0; RFMS - OS30 MVS	10, HP-UX 10.20	Open VMS / OS/390 MVS/ESA	HP-UX 11, NT4.0, Win2000	HP-UX	Win2000 (siebel), HP- UX (database)	Solaris 2.6, HP UX Solaris 11.0, NT4.0, Oracle 8.1.6	is 2.6, HP UX Solari NT4.0, Oracle 11.0, N 8.1.6	12.6, HP UX Solaris 2.6, HP UX IT4.0, Oracle 8.1.6 Solaris 2.6, HP UX	OS 390	IBM CMOS 88	NT 4.0	HP-UX	Server for fut	dows NT 4.0 sp6a with plans Hi ure upgrade to vs 2000 Server	P-UX 11, Oracle Financials			Solaris 8	Solaris 8	HP-UX 11.0, Solaris 2.6.1	Linux	MVS/ESA	Data: OS 390 2.8; Web: NT 4.0	MS SFA-PIN: HP-UX/Unix NSLDS: OS/390 2.8, MS NT 4.0 server, IE DB2 5.1	M NT 4.0/Oracle	HP/UX 10.2, MS NT 4.0 server	IBM CMOS 161/3390 HP900i	0 NT 4.0	HP-UX 11.0, Sun Solaris 8, MS Windows NT Server 4.0, Oracle 8i 8.1.6 OS/390, DB2 5.1
Application Server		Pell - NT 4.0; RFMS - OS30 IBM CICS 4.1	Allaire JRUN application server; database Informix 7.31		Compaq Application Servers	77	Win2000 (Siebel)	NT 4.0 SP6a NT	7 4.0 SP6a NT	4.0 SP6a NT 4.0 SP6a	N/A				Орга	a Acorde 2.2 Hi	PI10 and HPL11, acle Apps 11.0.3			BEA Weblogic	BEA Weblogic	Websphere 3.5; Viador Portal/Allair Jrun	Cold Fusion	η	Data/App: IBM CRS 4.	1 SFA-PIN: WebSphere IBM CICS	2 Compaq Prollant 1850R	Web Citrix server			Websphere 3.5 SFA-PIN: WebSphere
Web server		Pell - NT 4.0/IIS, CA;CoolG	en HP-9000 K570, HP-UX 11.0; iPlant Webserver	15 Compaq Proliant Servers	Nia	η	TBD - Win2000 willS OR iPlanet on Solaris	IIS 4.0	IIS 4.0	IIS 4.0 IIS 4.0	NIA				Micr	osoft IIS 5.0	7			Apache	Apache	IBM HTTP server 1.3.6	Apache	77	IIS 4.0	IBM HTTP server		IIS 4.0			IBM HTTP Server 1.3.12 SFA-PIN: IBM HTTP serv CPS: IBM CICS 4.1
External systems utilizing authoritization	None	Pell - RFMS, RACF 2.4			DLSS via processor code	77	Interfaces with NSLDS, DLSS, DLCS, CPS/WAN, eCB	No	No	No No			PEPS for Oracle Listener File and Valid School Address			No	?			Various ASP provider hosting application data	Various ASP provide hosting application da		None	Yes. The Student Authentication Network (STAN) project utilizes systems that are on the Intermed in a firewall protected De-Mistanced Zone (DMZ). Servesis located in the DMZ are monitored to ensure that the latest security patches are installed regularly, only required services and protocols are installed, and informed traffic to the servers is controlled by a firewall.		IBM RACF 2.2	n.a.	eApp, EDPUBS (school address file)	Receives mailting addresses from PEPS No		? ?
alpolesik .	Admin by SFA, Tier 1 Support by AFSA-Niagra Falls, Operations TSYS, VDC	y Federal Pell Grant Hotline at 800-4PGRANT or 1-800-47 7268	t 1- 4- DLOS Web Help Desk	ACS/AFSA (Utica, NY and Bakerofield, CA)	ACS and AFSA's support organization in Rockville, MD; Utica, NY and Bakersfield, CA	DLCS Help Desk	Consistent Answer consolidated held desk	Modpartner Mo	od Partner Mo	d Partner Mod Partner	Level 1 - Raytheon, Level 2 CSC	Level 1 - Raytheon, Level CSC	Case Management Team are Tier 1, Tier 2 System Administrator			M	od Partner, CSC	see FMS	see FMS	Jamoracker Service Center	Jamoracker Service Center	Customer Service Call Center (CSCC) in Schools Channel	System manager, ORNL	PIC (NCS Pearson)		PIC (NCS Pearson)	ROH Incorporated, VDC Help Desk	Admin by SFA, Operations by CSC	n.a.		CB Call Center & NCS Pearson PIC (NCS Pearson)
ercentage of calls related to coess problems	30,000 expected calls per month; 20%?? for login/access questions			n		77	n.a., - future systems						Volume of calls is low			0	In average 20%			Less than 1 percent	Less than 1 percent		few	Not available but reasonable estimation would be 20%. Reported problems are forgotten passwords, password accounts locked, RACF revoked IDs.			20%; Loss of server access most common problem	1 to 2 per week	n.a.		
perations costs to operate/administer access ontrol processes and operations	77			77									Costs unknown							\$200K	\$200K			Not identified			T&M contract with \$199,000 ceiling for all OCTS application and Desk	??			
Enrollment Helpdesk Administration																				included included included included	included included included						operations				
Development Maintenance								MicroStrategy Micr	proStrategy Mic	roStrategy			PEPS and Oracle							included	included						IP Address, Username and				
dministrative authentication nechanism	COD database	Pell - RFMS, RACF 2.4		Username and password matching	Username and password matching	Username, Password matching	Siebel iPlanet directory	datamart; Oracle datam DBMS	mart; Oracle data DBMS	roStrategy nart; Oracle DBMS MicroStrategy datamart; Oracle DBMS	S RACF	RACF	PEPS and Oracle Listener File to validate OPEID and TIN		Windo	ws NT domain FI security	MS Oracle User FM repository	IS Oracle User repository	FMS Oracle User repository	Jamcracker's LDAP allowed these rights	Jamcracker's LDAP allowed these rights	IFAP Oracle DBMS	IAM database	Usemame and password matching	RACF	SFA PIN Username, Password o SFA PIN Site	password client to server match	PEPS Database			Usemame, Password
ransactions provided by system sparactions are flabilities	77 No			77	Business processes related to Borrower Service & Louin Counseling cell and Counseling cell and Counseling cell and Counseling cell and Counseling Counseli	77		Retrieval mode access to data for coperformance valuation, risk accessment, and accessment, and program compliance program	rileval mode sis to data for reformance paulation, ride wall assement, and mr compliance progra	Retrieval mode access to data for periorization retrieval mode access to data for performance station, risk assessment, and program compliance	Maintenance of outstanding financial debt includes but not lented to management, billing, and collectors		Information collected through this website is stored in PEPS and is available to OIG, OMB, OGC users given access to PEPS							Complete audit trail of all accords  Ves. contract/SLA	Complete audit trail of all actions  Yes. contract/SLA	T No.	No	Data Drin, Inspiri, Editing Proceeding, Production of Station Loan Application. Date ID Passessel Name, Date of Birth, Social Security Namber, etc.,			User access the Case. Account and Admity work environments. Users with win deein protocol can also create and attach various work files from non-readiset applications to e-mail (Microsoft Ostock 2000) for transport to work locations files of the Case of the Case files of the Case of the Case files of the Case of the Case of the transport to work locations after the Case of the transport to work locations after the Case of the transport to work locations after the Case of the transport to work locations after the Case of the transport to work locations and the Case of the transport to work locations and the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the transport to work locations are the case of the case of the transport to work locations are the case of the case of the transport to work locations are the case of the case of the transport to work locations are the case of the case of the transport to work locations are the case of the case of the transport to work locations are the case of the case of the transport to work locations are the case of the case of the transport to the case of the case of the transport to the case of the case of the transport to the case of the case of the transport to the case of the case of the transport to the case of the case of the transport to the case of th				The hyper of samelation determination that application by the application by the application by the samelation to the determination to the samelation and the samelat
ager actions and nutrenticate users	No e-sign.			n	In addition to Key card access to building locations, LAN lids and Application lids and passwords authenticate users. Processor code on DLS is used to account for user action. Processor Code is stored in contact and transaction history for CSR accountability.	77		Manual 8	Manual	Manual Manual	?										Yes, identification, authentication and provisioning controls f Jamoracker and each ASP	None. Registration requires FN, LN, or Organization, Type, email address	SFA/ED Employee iccess only; Case an agement specific	System Security Application Security Database Security Physical Security Security Clearances Audit Software		Provide PIN before submission	No resident information about previous sign-on maintained to permit bypassing of logon requirements.				PIN 8 TG# Provide PIN before submission
ise of and protections for Privacy	No Private Act data. Contains Confidential Data	Private and confidential	Private and confidential	Privacy Act and Confidential Data	Privacy Act and Confidential Data	Private and confidential	Privacy data	Yes	Yes	Yes Yes	Yes, Privacy Act and Confidential	Yes, Privacy Act and Confidential	Confidential and Proprietary data		Con Pro	fidential and Corietary data F	Confidential and Confidential and Proprietary data	onfidential and roprietary data	Confidential and Proprietary data	Yes, contract/SLA	Yes, contract/SLA	No	Confidential	Privacy Act and Confidential data	Privacy Act and Confider data	rial Yes	Privacy and confidential	Confidential/Proprietary data; No Privacy Act data			No Yes

Commit Signin Logon Analysis
(F) Single Sign on Requirements

					Portals			Virtual Data Center	Future Systems	Single Sign-on
SFA - Single Sign-on	DLCS (Direct Loan Consolidation System)	DLSS (Direct Loans Servicing System)	FAFSA on the web	FAA Access On- line	Schools Portal	Financial Partners Portal	Students Portal	VDC	submittal of audit reports and financial statements	
Data Collection Status	Complete	Complete	Complete	Complete	Complete User ID only used	Complete	Complete	Complete		Planned
General	Direct Loan consolidations	Borrower: Direct Loan Servicing (eServicing)			for customizing Portal homepage. Not required.	Under development	Under development	System infrastructure		Single sign-on to SFA applications by enrolled users
Contact IPT contact	Robert Laurence	Robert Laurence	Robert Laurence	Robert Laurence		Pam Eliadis	Robert Laurence	Ray Thomas/Gary Adams		Neil Sattler
Business Process Business Owner			Jennifer Douglas		User Portal Kay Jacks 202- 377-4286	User Portal  John Reeves	User Portal  Jennifer Douglas			User Access Security Steve Hawald
System Owner System Manager (SM)	Denise Leifeste, (202) 377- 3293 Denise Leifeste, (202) 377- 3293	Dan Hayward (202) 377- 3207 Dan Hayward, (202) 377- 3207	Jeanne Saunders, (202) 377-3246 Jeanne Saunders, (202) 377-3246		Colleen Kennedy, (202) 377-4119		Mary K. Muncie 202- 377-3202 Mary K. Muncie 202- 377-3202	Keith Wilson, (202) 377 3591		
System Security officer (SSO)	Yvette Payne, (202) 377- 3295	3207 Schonda Piper, 202-377- 3275	Yvonne Somerville (acting), 202-377-3247		Lloyd Nicholson, (202) 377-4336		Yvonne Sommerville 202-377-3202	Jim Cunningham, 202- 377-3577		
Logon (Credentials) Usemame	SSN + First two letters of last name + Date of birth	SSN + First two letters of last name + Date of birth	SSN + First two letters of last name + Date of birth	SSN + First two letters of last name + Date of birth	School Portal Username	FP Portal Username, only used to access personalization page	Student Portal Usemame, only used to access personalization page			
Minimum length	9 numeric+2alphanumeric+8n umeric	9 numeric+2alphanumeric+ 8numeric	9 numeric+2alphanumeric+ 8numeric	9 numeric+2alphanume ric+8numeric	N/A	6	6			
Maximum length	9	9	9	9	8 characters	9	9			
Syntax rules	Must not be empty, 9 characters long	Must not be empty, 9 characters long	Must not be empty, 9 characters long	Must not be empty, 9 characters long	First letter of first name + (up to) six letters of last name + number (assigned incrementally for matching strings)	Must not be blank, must be between 6-9 alphanumeric characters long, check for profane words	Must not be blank, must be between 6-9 alphanumeric characters long, check for profane words			
Password PIN other	SFA-PIN	SFA-PIN	SFA-PIN	SFA-PIN	School Portal Password, user selected	FP Portal Password	Student Portal Password			
Lifetime	Expire after 6 months of inactivity; else valid indefinitely	Expire after 6 months of inactivity; else valid indefinitely	Expire after 6 months of inactivity; else valid indefinitely	Expire after 6 months of inactivity; else valid indefinitely	never expires	Expire after 6 months of inactivity; else valid indefinitely	Expire after 6 months of inactivity; else valid indefinitely			
Minimum length	4	4	4 char	4	N/A	6	6			
Maximum length	6	6	6 char	6	16 characters	9	9			
Symbox rulies	Must not be blank, must be digits	Must not be blank, must be digits	Must not be blank, must be digits	Must not be blank, must be digits	none	Must not be blank, must be between 6-9 mixed alphanumeric characters and contain at least two letters, at least one uppercase letter, no special characters or repeating characters are allowed	Must not be blank, must be between 6-9 mixed alphanumeric characters and contain at least two letters, at least one uppercase letter, no special characters or repeating characters are allowed			
Previous passwords stored	No	No	No	No	no	No	No			
System where credentials are stored	SFA-PIN site	SFA-PIN site	SFA-PIN site	SFA-PIN site	Oracle database	Oracle DB located at the VDC	Oracle DB located at the VDC			
General	PIN not retrievable	PIN not retrievable	PIN not retrievable	PIN not retrievable						
Guest accounts	No	No	No	No	N/A	No, but most pages accessible without authentication	No, but most pages accessible without authentication			
Disable when inactive	Yes, after 6 month	Yes, after 6 month	Yes, after 6 month	Yes, after 6 month	Yes, upon receipt of undeliverable email	After 6 month	After 6 month			
Credential data elements		Username, PIN (Username consists of SSN, DOB, LN)	Username, PIN (Username consists of SSN, DOB, LN)	Username, PIN (Username consists of SSN, DOB, LN)	First name, last name, email address, user selected password	Username, Password	Username, Password			
Single or multiple logans for one user	Single	Single	One PIN per user	Single	Multiple	No	No			
Different credentials for user groups	No	No	Students, Parents only	No	No	N/A	N/A			
Encryption of credentials	Yes, two-way	Yes, two-way	40/56/128-bit encryption; One-way	Yes, two-way	Yes, one-way for password	Yes, One way	Yes, One way			
Comments  User management		borrowers are authenticated via VRU during calls				If a temporary password is created that password will expire within a few days. If it is used to logis then it will immediately expire and the user is forced to change their password.	If a temporary password is created that password will expise within a flow days. If it is used to logist then it will immediately expise and the user is froated to change their password.			
Enrollment	SFA self service PIN web site	SFA self service PIN web site	SFA self service PIN web site	SFA self service PIN web site	Web self service, no validation	Automated	Automated			
Enrollment data elements	SFA-PIN	SFA-PIN	SFA-PIN	SFA-PIN	FN, LN, email address, password					
Username creation automated  System generates initial	Yes	Yes	Yes, utilize preexisting items - SSN, DOB, LN	Yes	Yes	User can set initial password and username. Forgotten passwords trigger an email with a temporary password	User can set initial password and username. Forgotten passwords trigger an email with a temporary password			
System generates initial Password User is forced to change initial Password	Yes, but changeable No, mail via USPS to recipient	Yes, but changeable  No, mail via USPS to recipient	Yes, but changeable  No, mail via USPS to recipient	Yes, but changeable No, mail via USPS to recipient	No No	No No	No No			
Removal  Average time before removal	Immediately	Immediately	Immediately	Immediately	None removed	Immediately	Immediately			
Manual or automated	?	?	?	7	Manual	Automated	Automated			

Figs. 3

Current Single Sign-on Requirement
IPT Single Sign-on Requirement

Column											
### Study Supple Supple						Portals			Virtual Data Center	Future Systems	Single Sign-on
The control of the	SFA - Single Sign-on	DLCS (Direct Loan Consolidation System)	DLSS (Direct Loans Servicing System)	FAFSA on the web	FAA Access On- line	Schools Portal	Financial Partners Portal	Students Portal	VDC	submittal of audit reports and financial	
The content of the	User groups, where stored	PIN DB (Oracle DB housed at VDC)	PIN DB (Oracle DB housed at VDC)		PIN DB (Oracle DB housed at VDC)	N/A	No groups	No groups			
Comment   Comm	Plassword administration automated	Yes	Yes	Yes	Yes	Self Service on web	Yes, via Web	Yes, via Web			
Transact	Number of enrolled users	27,274,093 including other SFA-PIN sites	27,274,093 including other SFA-PIN sites	approx. 5 million	27,274,093 including other SFA-PIN sites	13,197, however many user have multiple	?	7			
March   Marc	Session management					registrations					
Decision for parameter   Decision for the Color (No. 100)   Decision for the Color (	Timeout	30 minutes	30 minutes	30 minutes	30 minutes	No	30 minutes of inactivity	30 minutes of inactivity			
No.	Logout button	Yes	Yes	Yes	Yes	Yes		No			
March   Marc	Mechanism for session management	Oracle WAS (Session DB)	Oracle WAS (Session DB)	Oracle WAS (Session DB)	Oracle WAS (Session DB)	N/A	WAS Oracle session DB/Websphere/Strut s	WAS Oracle session DB/Websphere/Struts			
Access (minuted by security)   No.		No	No	No	No	Yes	No	No			
The or challenge access   Title and 108   Ti		No, 24X7 availability	No, 24X7 availability	No, 24X7 availability	No, 24X7 availability	No	No	No			
Contract	Access limited by location	No	No	No	No	No	No	No			
CS   Parson   PN		Web and IVR	Web and IVR	Internet access only. WAS (web application server) Oracle session database	Web and IVR	Web	FPs will use the Internet	Students will use the Internet			
Contract Control   Absorbance   September   Septembe	Environment Infrastructure										
Cycle of System Control (Control (Contr	Data Center Location	NCS Pearson - PIN database; VDC - Web Application	NCS Pearson - PIN database; VDC - Web Application	NCS Pearson - PIN database; VDC - Web Application	NCS Pearson - PIN database; VDC - Web Application	VDC					
Cycles fig System	Hardware platform	SFA-PIN: HP DLCS: HP		HP, Sun	HP	HP 9000 T 600	Sun E3500	HP, 7			
With server GFA-PN BBI HTTP server BBI HTTP se	Operating System	SFA-PIN: HP-LD/Unix DLCS: HP-UX 11.0, Informix 7.31	DLSS: Compaq Alpha Once VMS 7.2 Mindows	HP-UX 11.0, Solaris 8, Oracle 8i 8.1.7	HP-UX/Unix	HP/UX 11.0	Solaris 2.6	HPUX			
Enternal systems disting authorization and final states of the state of the states of	Application Server		WebSphere	Websphere 3.5	WebSphere	Viador Portal	Websphere	Websphere			
External systems at library authorization-burden-burden  PC (NCE Pleases)		SFA-PIN: IBM HTTP server DLOS	IBM HTTP server	IBM HTTP server 1.3.12	IBM HTTP server	IBM HTTP server	IBM HTTP server	IBM HTTP server			
PC (NCS Pearson) Parson CSPs Parson	External systems utilizing authentics florvlauthorization	?	?	SFA-PIN web site	?	None	N/A	NIA			
Count to operate and operations  Fire Configuration  Fire Configur		PIC (NCS Pearson)	PIC (NCS Pearson)	Information Center, M-F	PIC (NCS Pearson)	Center 1-800-433 7327; Email at sta customer sun	тво	TBD			
Total				77			N/A	NIA			
Advancement Control Co	Costs to operate/administer access			77			N/A	N/A			
Consideration Administration Administration Determine, Password Username, Password Conditions NA											
Transactions provided by system	Administration Development Maintenance						N/A	N/A			
Transactions provided by system	Administrative authentication mechanism	Username, Password	Username, Password	Username, Password	Username, Password	Schools Portal Database	N/A	N/A			
Transactions provided by system  Transactions provided by system  Courselons FFRS on the NAIA, Budder Access, FFRS on the NAIA, Budder Access, Frederic Course  Logical actions and faibliness  Transactions provided by system  NA NA NA NA NA  NA NA NA  NA NA NA  Logical actions and faibliness  Transactions for access fine in a submission of the NAIA NA  NAIA NAIA NAIA NAIA  Logical actions and faibliness  Transactions and faibliness  Transactions for access fine in a submission of the NAIA NAIA NAIA NAIA NAIA NAIA NAIA NAI	Legal										
Enlaguada to authenocate users Prociós PRI talibra subressano del prociós PRI talibra authenocate users Prociós PRI talibra authenocate users authenocate us				FAFSA on the Web,		N/A	N/A	N/A			
Safeguards to authensicate class  Polide PN before authensicate class  Polide PN before authensicate class  Polide PN before authensicate authensica	Legal actions and liabilities			77		N/A	N/A	N/A			
Use of end proscioles for Phasicy Act and conditional humanities date  Ves  Ves  Ves  Ves  Ves  Ves  Ves  No  No  No  No  No  No  No  No  No  N	Safeguards to authenticate users	Provide PIN before submission		access. E-sign is a separate section after the on-line FAFSA form.	Provide PIN before submission	None	N/A	N/A			
	Use of and protections for Privacy Act, and confidential/sensitive data	Yes	Yes	Yes, data is confidential.  Data protected by Privacy Act. Data not available to public	Yes	No	No	No			

Page 4